Adherence to forensic procedures

Mistakes that were made

1. Laptop and phones had been left out and plugged in, instead of being securely out of sight.
2. Insurance claim was not made.
3. Serial numbers of laptops and phones were not taken/recorded as well as IMEI identifiers of smartphones.
4. No realisation of what other items may be missing until a search for the laptop took place.
5. No attempt at asking for witnesses and their statements from anyone in the area including security, maintenance workers and cleaners.
6. Leaving employee cards out of sight, making it easier to steal.
7. No checks to see if employees still possess their cards.
8. No check on card system to see if there is abnormal activity
9. No checks with security to see if they saw anything strange, while checking the premises.
10. No check on network to see if access could've been granted this way
11. No police investigation such as forensics and foot/fingerprint took place, to catch potential suspects.
12. Data was not remotely wiped from the laptop using Find My Device software, even though the tool offers this facility.
13. Laptop was not remotely password locked using Find My Device software, even though the tool offers this facility.

Improving forensic procedures and the current protection measures

Recommendations

1. Update physical security policy for the devices. For example, if BCTAA frequently stores its devices in an unsecured area which is in sight, it could attract potential robberies. Policy changes should be implemented, so that BCTAA stores its devices securely, such as a key operated cupboard, or padlocked/pin protected cupboard, to protect these devices from theft. These cupboards come at an expense though. Staff should be trained to ensure they put the devices back into these cupboards when they are finished. Network components must also be kept secure, and only accessible by authorised people, to limit physical access and attacks to the network. A requirement should be that employees and staff should be required to sign in and sign out with their cards, instead of one employee opening the doors for everyone to go out. This action meant that it was impossible to look at the door logs and decipher who left the premises and who remained on sight. This would allow BCTAA to know who is present in the premises and who is not. This would limit theft, as all employee's movements will be accounted for.

2. Update security policy. If the current BCTAA policy doesn't include the security and requirements of a password on the network, it should be edited to include this. BCTAA must enforce this password policy on all staff and clients, to ensure that their data is as protected as possible. Having strong passwords which are complex, would limit an attacker from guessing a password and gaining access. A policy could be to make it mandatory to frequently change your password after a given time period. This would come at no additional cost, and would enforce data security.

3. Scanning procedures. All staff and guest mobile devices and staff accessing the network remotely, should be scanned before they are allowed to connect to its respective wireless access point and ultimately the network. Scanning these devices would better protect the network from intrusion as well as infection and would help to limit attacks to the door control system, which is connected to the network. Scanning procedures comes at a low cost, as antivirus software usually includes this as part of its package.

4. BCTAA should ensure that mobile devices should not allowed to re-connect to the wireless access point & Wi-Fi without requiring a password. Otherwise people who have previously been in the BCTAA premises will always be connected to the network when they are near premises and their device picks up the connection. This is unsafe and could potentially lead to unauthorised access to the server and access to its files. This can be carried out by randomly generating access point passwords or requiring a user to login to the network with certain credentials. It can also be achieved by limiting a certain device's time that they have access to the network. This may be reasonable in terms of cost, as many modern Wi-Fi routers allow this functionality and the ability to limit devices and change passwords. However, it is likely to be time consuming to frequently do this manually.

5. Evidence preservation. Copies of the door logs should be made and kept. This is to ensure that different people such as police, forensics, Baljinder and the EH management company all have a copy of the document and can analyse it for themselves and move forward with the investigation. Having copies of the logs means that if the thieves did return and tried to delete the logs, there is still a backup and evidence. As more activity is recorded, the logs are likely to be overwritten, so copies must be made before this occurs. This is relatively cheap to do, as it would be cheap to print out copies of the logs.

6. Evidence preservation. Copies of the meeting summary must be made and kept. This is to ensure that a record of what took place in the meeting and everything that was said is made. This would help in the investigation and would ensure that everyone is informed of what is going on and the current progress. Different people such as police, forensics, Baljinder and the EH management company would benefit from the meeting summary and can analyse it for themselves to keep up to date and learn more about what happened and try to piece together a sequence of events and move forward with the investigation. Having copies of the logs means that there is meeting notes and evidence of this, so that if someone forgets what was said in the meeting, they can remind themselves. This is relatively cheap to do, as someone in the meeting would write down everything that is said and then photocopy this document or record the meeting with a device such as their personal smartphone and share the recording via email or Bluetooth to other members of the meeting. Baljinder should also write down a copy of his account, so that he can share this is part of the investigation.

7. Evidence preservation. The laptop tracking report should be preserved and kept. This is so that a copy can be shared with the insurance company to help with their claim as well as with the police in order to aid the investigation. There should be someone to forward this report to these two groups to help BCTAA recover their losses. It would come at a low cost to copy this report and forward it to the two groups.

Improving the security documentation

General weaknesses and omissions.

1. Once a theft is discovered, it is not clear what should happen next. "etc." is not clear enough and doesn't tell staff what to do correctly. The policy should be improved, so that the terminology and the wording in this policy give clear, logical instructions for a staff member to report a theft. It is also not clear enough how they will get the serial numbers of the devices lost.

2. Baljinder is responsible for the network. However, a team leader must ascertain if the device is actually stolen or just misplaced. It is not clear who this team leader is. It is not clear if this refers to Baljinder or another person who is part of the BCTAA team. No contact details of this team leader are also on the policy. To improve the policy, the contact details of Baljinder or the team leader should be included, such as their location and where to find them as well as company email or telephone number, where they can be communicated with.

3. The policy also gives out no instructions about preserving evidence or securing the scene of an incident, which would aid the investigation regarding the incident. This must be included in the policy. For example, for each procedure, there should be instructions such as:

    Hardware theft
    1. Ensuring CCTV footage is analysed and downloaded if possible.
    2. Take up eye witness accounts and statements from staff and people who were near the location.
    3. Keep staff and visitors away from the incident location.
    4. Ensure that tracking software on the devices is immediately turned on and remotely locked and wiped, to prevent data theft and unauthorised access.

    Theft of Data
    1. Ensure that all logs such as network and Wi-Fi access and activity logs are produced and kept securely to aid the investigation.
    2. Ensure that a full network scan takes place to ensure there are no unauthorised devices on the network.

    Infection of IT systems with Malware
    1. Run antivirus software and produce results report ready for analysis and review. Delete the suspicious file and run a full scan to ensure all traces of the virus are gone.

    Unauthorised access to BCTAA systems
    1. Analyse firewall activity
    2. Assess if there are any unauthorised devices on network.
    3. Check user and device activity on network.

4. There is no review and evaluation of the incident, as the policy suggests. Following processes and procedures should've occurred, depending on the incident type.

Theft of IT equipment

The USB sticks which were stolen should have been logged and reported to Baljinder and to senior management within BCTAA. Especially if the USB's contained highly sensitive data. Then this would need to be reported to the police and insurers, as client's data is at risk and could impact them. The laptops and phone thefts should have been reported to the police and insurers too, no matter the age of the

device. However, this would increase the cost of insurance, due to the no claims discount ending and BCTAA would likely have to pay high insurance excess fees, in order to get replacements and even higher for future claims.

Theft of Data

Data which has been stolen or lost, would have to be reported to the relevant authorities. This is because businesses must comply with the Data Protection Act, and must inform the relevant bodies, if there has been a breach and confidential and highly sensitive data has been accessed unauthorised. The senior manager and public relations officer would be involved in this process; however, they are not named and their contact details provided.

Infection of IT systems with Malware

Antivirus software running on the BCTAA systems would pick up malware and viruses. These would be logged by the software, but would also need to be manually logged by the team leader. The policy says the infected system must be isolated as soon as possible. This means that the affected computer would no longer be used until the malware is contained and quarantined. This is not necessary, and would only be necessary to shut them down the computer if the virus spread to other devices on the network and if it could not be contained & isolated.

Unauthorised access to BCTAA Systems

The team leader would have to investigate the incident and identify how unauthorised access was gained. The team leader would ensure that this access is never granted again and that the systems are as secure as possible. However, it is unclear what the team leader is supposed to do. "The team leader will take whatever action is required to prevent future occurrences (change passwords, etc.)" this language is informal and doesn't give clear information of what the team leader is supposed to do, such as when to log the activity down, who and when to contact the relevant authorities and bodies and who to inform within the company.

The document could also be improved by being extended to cover the full range of potential security incidents and protocols and procedures that must be followed, in order to deal with these.

Specific weaknesses of the Theft of IT equipment section.

"Once a theft is discovered, collect as much information as possible (location and type of equipment, serial numbers, when it was last seen etc.)."

The language used in this section is too vague and unclear. It doesn't state who should collect the information regarding the device and who to present this information and findings to. The use of "etc." is also informal and also doesn't present an instruction on what to do.

"The team should review the incident and implement procedures to prevent future losses".

Another unclear and vague statement. It doesn't state who is part of the team and who would be involved in the decision making process regarding these decisions. The policy should be improved to show who would be involved in determining and implementing these procedures. "The team" could refer to anyone within BCTAA such as ordinary staff and clients, as well as management.

“If the item is confirmed as stolen, the team leader must inform the senior manager and public relation members of the team who will determine if the police need to be involved and who will run the internal enquiry.”

The language is also not as concise as it could be. The section does not identify who and where the public relation members are and where they can be found. Also doesn’t have any information regarding police use for insurance purposes and for investigations. Also no information about what to do with the stolen device, such as activating tracking software and remotely wiping and clearing data held on it and using these reports as part of the investigation.